IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Attorney Docket No.: **01-1518**

Appl. No.: **10/616,449**

Appellants: **Robert T. Baum**

Filed: **July 8, 2003**

TC/A.U.: **2434**

Examiner: **Jacob Lipman**

Confirmation No.: **1038**

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Further to the Notice of Appeal filed on August 27, 2009, the appellant requests that the Board reverse all outstanding grounds of rejection in view of the following.

TABLE OF CONTENTS **Page**

I. Real Party In Interest

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

II. Related Appeals and Interference

There are no related appeals or interferences.

III. Status of Claims

Claims 1, 6, 8, 14-15, and 19-31have been previously canceled.

Pending claims 2-5, 7, 9-13, 16-18 and 32-37 are finally rejected and are being appealed herewith.

IV. Status of Amendments

No amendments have been made subsequent to the final office action dated May 28, 2009, and no new matter has been introduced.

V. Summary of the Claimed Subject Matter

The following summary of the presently claimed subject matter indicates certain portions of the specification (including the drawings) that provide examples of embodiments of elements of the claimed subject matter. It is to be understood that other portions of the specification not cited herein may also provide examples of embodiments of elements of the claimed subject matter. It is also to be understood that the indicated examples are merely examples, and the scope of the claimed subject matter includes alternative embodiments and equivalents thereof. References herein to the specification are thus intended to be exemplary and not limiting.

Independent claim 2 recites a security method for use in a communication system, the security method comprising:

receiving an IP packet including a source address and a destination address (this is supported, for example, by Figure 19, elements 1904, 1906, and 1908; and page 56, lines 9-14 and page 57, lines 5-10);

obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address (this is supported, for example, by Figure 19, 1918; and page 57, lines 19-22), and wherein determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with edge router and port information (this is supported, for example, by Figure 13, 1316; and page 40, line 28 to page 41, line 2);

determining, as a function of the obtained physical location information, an action to be taken (this is supported, for example, by Figure 19, 1910; and page 60, lines 11-16), wherein determining an action to be taken includes:

comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided (this is supported, for example, by Figure 17, 1712; and page 51, lines 20-24).

Independent claim 7 recites a security method for use in a communication system, the security method comprising:

receiving an IP packet including a source address and a destination address (this is supported, for example, by Figure 19, elements 1904, 1906, and 1908; and page 56, lines 9-14 and page 57, lines 5-10);

obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address (this is supported, for example, by Figure 19, 1918; and page 57, lines 19-22), including transmitting a location information request message including the source address of the received IP packet (this is supported, for example, by Figure 19, 1916; and page 57, lines 14-19) and receiving in response to said transmitted location information request message, information corresponding to the location of the user device (this is supported, for example, by Figure 19, 1918; and page 57, lines 19-22);

determining, as a function of the obtained physical location information, an action to be taken (this is supported, for example, by Figure 19, 1910; and page 60, lines 11-16), and

determining the location of the user device from edge router and port information obtained from an edge router (this is supported, for example, by Figure 13, 1314; and page 40, line 25 to page 41, line 2), wherein the determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with said edge router and port information (this is supported, for example, by Figure 13, 1316; and page 40, line 28 to page 41, line 2).

Independent claim 9 recites a security method for use in a communication system, the security method comprising:

(a) receiving an IP packet including a source address and a destination address (this is supported, for example, by Figure 19, elements 1904, 1906, and 1908; and page 56, lines 9-14 and page 57, lines 5-10);

(b) obtaining physical location information indicating the location of a user device which is the source of said IP packet (this is supported, for example, by Figure 19, 1918; and page 57, lines 19-22), by:

(i) transmitting a location information request message including the source address of the received IP packet (this is supported, for example, by Figure 19, 1916; and page 57, lines 14-19),

(ii) receiving in response to said transmitted location information request message, information corresponding to the location of the user device (this is supported, for example, by Figure 19, 1918; and page 57, lines 19-22) determined from edge router and port information obtained from an edge router and a device identifier associated with the source address of said IP packet (this is supported, for example, by Figure 13, elements 1308 and 1316; and page 40, lines 8-11 and line 28 to page 41, line 2);

(iii) performing a database lookup operation to retrieve a geographic location stored in association with said edge router and port information (this is supported, for example, by Figure 13, 1316; and page 40, line 28 to page 41, line 2), and

(iv) comparing the received device identifier to a list of device identifiers corresponding to stolen devices (this is supported, for example, by Figure 19, 1920; and page 57, lines 22-28),

and

(c) determining, as a function of the obtained physical location information, an action to be taken (this is supported, for example, by Figure 20, 2016; and page 58, lines 4-12).

Dependent claim 11 recites the method of claim 9, further comprising:

generating a message indicating the detection of a stolen device when said comparing step detects a match between the received device identifier and a device identifier in said list of device identifiers corresponding to stolen devices (this is supported, for example, by Figure 20, 2020; and page 58, lines 6-12).

Dependent claim 12 recites the method of claim 11, wherein said generated message includes information indicating the geographic location where the identified stolen device is being used (this is supported, for example, by page 58, lines 13-18).

Independent claim 16 recites a security device for use in a communication system in which IP packets are transmitted, the device comprising:

means for receiving an IP packet including a source address and a destination address (this is supported, for example, by Figure 17, 1706 and Figure 1, elements 106 and 108; and page 50, line 30 to page 51, line 1, and page 3, lines 9-10);

means for obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address, wherein determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with edge router and port information (this is supported, for example, by Figure 17, 1712, and Figure 11, elements 1164 and 1162; and page 56, lines 8-9, page 57, lines 14-22, and page 40, line 28 to page 41, line 2); and

means for determining, as a function of the obtained physical location information, an action to be taken (this is supported, for example, by Figure 17, 1712; and page 56, lines 8-9, and page 60, lines 11-16);

a database of physical location information listing physical locations authorized to obtain access to said service (this is supported, for example, by Figure 18, elements 1804 and 1806; and page 60, lines 21-30); and

wherein said means for determining an action to be taken includes a comparator for comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided (this is supported, for example, by Figure 17, 1712; and page 60, lines 11-30).

Independent claim 32 recites a location verification method, the method comprising:

receiving an IP packet including a source address and a destination address (this is supported, for example, by Figure 19, elements 1904, 1906, and 1908; and page 56, lines 9-14 and page 57, lines 5-10);

determining from said source address the physical location from which said IP packet was sent prior to delivery of the packet to the destination address (this is supported, for example, by Figure 19, 1918; and page 57, lines 19-22);

comparing the determined physical location information to expected information indicating the expected source of an IP packet (this is supported, for example, by Figure 21, 2110; and page 64, lines 9-14); and

determining a reporting error when said determined physical location information does not match the expected physical location information (this is supported, for example, by Figure 21, 2118; and page 67, lines 6-10).

Independent claim 36 recites a location verification method, the method comprising:

receiving an IP packet including a source address wherein said IP packet is transmitted from a bracelet worn by a parolee and wherein said IP packet includes parolee identification information (this is supported, for example, by Figure 17, 1752; and page 61, line 20 to page 62, line 2);

determining from said source address the physical location from which said IP packet was sent (this is supported, for example, by Figure 19, 1918; and page 57, lines 19-22);

comparing the determined physical location information to expected information indicating the expected source of an IP packet (this is supported, for example, by Figure 21, 2110; and page 64, lines 9-14);

determining a reporting error when said determined physical location information does not match the expected physical location information (this is supported, for example, by Figure 21, 2118; and page 67, lines 6-10);

transmitting a message including information on the determined reporting error to a law enforcement authority (this is supported, for example, by Figure 21, 2130; and page 67, lines 6-10, and lines 22-24);

including the determined physical location information in said message (this is supported, for example, by Figure 21, 2118; and page 67, lines 6-10);

identifying the device transmitting said IP packet from a MAC address determined from a database associating said MAC address with said source address (this is supported, for example, by Figure 21, 2106; and page 63, lines 21-27); and

including in said message information obtained from said IP packet identifying the parolee (this is supported, for example, by Figure 21, 2118; and page 67, lines 6-10).

Dependent claim 37 recites the location verification method of claim 33, further comprising:

determining if said IP packet was sent at a predetermined time during which a location reporting message was scheduled to be transmitted (this is supported, for example, by Figure 21, 2112; and page 64, lines 17-24).

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 2-5, 7, 9-13, 16-18, and 32-37 stand rejected.

Specifically, claims 2, 3, 5, 7, 16, 17 and 32 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Publication No. US 2004/0249975 to Tuck et al. (hereinafter "the Tuck et al. publication").

Claims 4, 18, and 33-35 stand rejected under 35 U.S.C. 103(a) as being unpatentable over the Tuck et al. publication in view of U.S. Patent No. 6,684,250 to Anderson et al. (hereinafter "the Anderson et al. patent").

Claims 9-13, 36, and 37 stand rejected under 35 U.S.C. 103(a) as being unpatentable over the Tuck et al. publication in view of the Anderson et al. patent in further view of U.S. Patent Publication No. US 2002/0165835 A1 to Igval (hereinafter "the Igval publication").

VII. Argument

The Appellant respectfully requests that the Board reverse the final rejection of claims 2-5, 7, 9-13, 16-18, and 32-37 in view of the following:

Rejections under 35 U.S.C. §102 and 35 U.S.C. § 103

Regarding rejections under 35 U.S.C. 102, "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art." *Brown v. 3M*, 265 F.3d 1349, 1351, 60 USPQ2d 1375, 1376 (Fed. Cir. 2001) (claim to a system for setting a computer clock to an offset time to address the Year 2000 (Y2K) problem, applicable to records with year date data in "at least one of two-digit, three-digit, or four-digit" representations, was held anticipated by a system that offsets year dates in only two-digit formats). See also MPEP § **2131.02**.< "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

Regarding rejections under 35 U.S.C. 103, the Examiner has a burden of stating a prima facie case of obviousness. Specifically, in view of recent case law, the MPEP provides:

The rationale to support a conclusion that the claim would have been obvious is that ***all the claimed elements*** were known in the prior art and one skilled in the art

could have combined the elements as claimed by known methods ***with no change in their respective functions***, and the combination yielded nothing more than predictable results to one of ordinary skill in the art. KSR, 550 U.S. at ___, 82 USPQ2d at 1395; Sakraida v. AG Pro, Inc., 425 U.S. 273, 282, 189 USPQ 449, 453 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 62-63, 163 USPQ 673, 675 (1969); Great Atlantic & P. Tea Co. v. Supermarket Equipment Corp., 340 U.S. 147, 152, 87 USPQ 303, 306 (1950). [Emphasis added.]

(MPEP § 2143) In addition, requiring the Examiner to show some reason for combining prior art references is considered important as noted in the United States Supreme Court's decision in KSR International Co. v. Teleflex, Inc.. Specifically, the Court in KSR stated that

It can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. [Emphasis added.]

(KSR International Co. v. Teleflex, Inc., 82 USPQ2d 1385, 1396 (2007); See also MPEP § 2143) As can be appreciated from the foregoing, the Court made clear that "a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." (Id. at 1389.)

Group I: Claims 2- 5 and 18

Claims 2, 3, and 5 stand rejected under 35 U.S.C. 102(e) as being anticipated by the Tuck et al. publication.

Claims 4 and 18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over the Tuck et al. publication in view of the Anderson et al. patent.

Claim 2 is representative of claim Group I.

First, the Tuck et al. publication identifies location by utilizing the "router NIC number", whereas **claim 2** recites "edge router and port information" to perform "a database lookup operation to retrieve a geographic location stored in association with the edge router and port information".

Second, Claim 2 is patentable because, among other things, it recites the features indicated below:

> *comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided*

The Examiner states on p. 2 of the final Office Action that the Tuck et al. publication discloses "information listing physical locations authorized to obtain access to a service for which security is to be provided ([0013])." However, the cited reference actually reads: "The information may for example relate to the department in which a user of the client node is registered and to their level of authority and security clearance". There is nothing about "physical locations authorized to obtain access" in this reference.

The Examiner then states on p. 5 of the final Office Action that:

> "the examiner points to 0017-0019 of Tuck, where Tuck discloses that the NIC is used as location information, and when it does not match any address in the database (expected locations), a security procedure is initiated."

Actually, [0017] of the Tuck et al. publication states (emphasis added):

> "Further preferably, the router determines whether a client node's **link layer address** is included in the database, and initiates a security procedure **when said address** is not in the database".

This is clearly using a "network address", rather than "the obtained physical location information" that is found in claim 2. Further, there is no teaching or suggestion of obtaining the "physical location information" in order to identify

"locations authorized to obtain access to a service for which security is to be provided". The Tuck et al. publication approach is **completely different** than claim 2.

Still further, the Examiner points on p. 5 of the Office Action to paragraph [0052] of the Tuck et al. publication. This paragraph refers to "physical network location (e.g. through VLAN ID and incoming router NIC number)". But even if this paragraph were to refer to a "geographic location" as opposed to a "network location", it still would not teach or suggest "comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided". Instead, [0052] refers to "router 2 is able to provide intelligent service delivery by making available relevant specific network and application services to selective users based on their user profile". This describes providing enhanced services to users, not "listing physical locations authorized to obtain access to a service for which security is to be provided".

The Examiner states on p. 2 of the Advisory Action dated August 5, 2009 that "the same employee will see different web pages in different physical locations". This again describes providing enhanced services to users, not "listing physical locations authorized to obtain access to a service for which security is to be provided".

Still further, in paragraph [0018] of the Tuck et al. publication (referred to by the Examiner on p. 5 of the final Office Action): "The system may also determine positional information of a client node **and may record the information in the database**" (emphasis added), as opposed to "listing physical locations authorized to obtain access to a service for which security is to be provided".

Then further in the paragraph "the client node may be provided with location specific services, such as location specific web page content". Again, this is far from "comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided".

Finally, in paragraph [0019], also cited by the Examiner on p. 5 of the final Office Action:

> "It would also be possible to assign other attributes to the link layer address that might previously have been associated with an IP address. This could include network resources, e.g. a printer and dynamic firewall rules (e.g. non-static IP)."

This section describes subject matter other than Appellant's claimed subject matter. First, this references "link layer address" as opposed to "geographic location". Second, the purpose is to allow the connection to be moved around, or provide it with network resources, such as a printer, as opposed to "comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided".

The Examiner states on p. 2 of the Advisory Action that "The claim states that the information is stored in association with edge router and port information, which Tuck discloses [as] outlined in the office action. The claim does not state that the database lookup is given the edge router and port information as search criteria".

Appellant disagrees that this is a correct characterization of "performing a database lookup operation to retrieve a geographic location stored in association with edge router and port information".

In addition, Appellant disagrees that the Tuck et al. publication discloses "stored in association with edge router and port information" or further "wherein determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with edge router and port information".

Furthermore, this still does not address "comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided", as argued above.

For at least these reasons, claim 2 is patentable over the cited references.

For at least the reason that they depend from allowable claim 2, claims 3, 4, 5, and 18 are patentable over the cited references. Therefore, the rejection of claims 2-5 and 18 should be overruled.

It should be noted that neither the Anderson et al. patent nor the Igval publication supply any of the missing features discussed above in relation to the Tuck et al. publication regarding claim 2.

Further, the Anderson et al. patent doesn't teach or suggest the determination of "physical location" recited in the referenced claim.

The Anderson et al. patent discloses an "estimated geographic location" based upon "a degree of confidence-factor weighted agreement within a plurality of geographic locations" (Abstract). This is accomplished by identifying the location of **a router** which is associated with the "machine" in question, not the location of the device itself. At col. 8, lines 14-20:

"Typically, most network addresses (e.g., IP addresses) are associated with a particular geographic location. This is because routers that receive packets for a particular set of machines are fixed in location and have a fixed set of network addresses for which they receive packets. The machines that routers receive packets for **tend to be geographically proximal to the routers** [emphasis added]".

Other methods employed by the Anderson et al. patent to estimate the approximate location of a device include:

1. Tracking ownership of blocks of IP addresses (col. 15, lines 33-35);
2. Tracking ownership of domain names (col. 15, lines 42-43);
3. Tracking autonomous systems of routers (col. 15, lines 46-50);
4. DNS Location record for a host (col. 15, lines 52-54);
5. Tracing the route of the data packet (col. 15, lines 55-60);
6. The "hostname" in a network address (col. 15, line 66-col. 16, line 1); and
7. "Demographic/Geographic Data" (col. 16, lines 5-7).

None of these methods teach "obtaining **physical location** information indicating the **location of a user device"**. At best, they are **guesses** at what **general vicinity** a device is **likely** to be found by identifying possible locations of **other devices** which **might be** nearby the target device.

Also, the Igval publication likewise does not teach or suggest the features argued above. The Igval publication teaches a method of estimating the approximate probable geographic location of a device, not "determining" the "physical location from which said IP packet was sent".

For example, paragraph [0027] states: "the locator application 128 may employ techniques such as sending 'homing' signals back and forth between the postage meter 140b and the data center 120 along different routes 165 through the Internet 160 and using the corresponding transmission **times** or other communications parameters associated with the homing signals to triangulate the physical location of the postage meter 140b" (emphasis added). Clearly, using **times of transmission**, with an estimate of the distance travelled, would not result in anything more than an **estimate** of possible locations, not "determining" the "physical location from which said IP packet was sent".

Group II: Claim 7

Claim 7 is patentable because, among other things, it recites the features indicated below (emphasis added):

> *obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address, including* ***transmitting a location information request message including the source address of the received IP packet and receiving in response to said transmitted location information request message, information corresponding to the location of the user device****; ...*
>
> *determining the location of the user device from* ***edge router and port information obtained from an edge router****, wherein the determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with said edge router and port information*

Claim 7 is patentable over the cited references for at least the reasons discussed above regarding the use of "port information obtained from an edge router".

The Examiner states on p. 3 of the final Office Action that "Tuck discloses using router and port information ([0073])". However, this paragraph states:

> "For any matching reverse session traffic that maps the client IP address (and additionally transport port number for NAPT) back, the router for the traffic forwarding uses the previously stored link information to generate the packet and transmit the packet to the client, and bypasses the normal route processing."

Clearly, this reference to "IP address" and "transport port number" in no way teaches or suggests "**determining the location of the user device from edge router and port information** obtained from an edge router".

For at least these reasons, claim 7 is patentable over the cited references.

Claim 7 also recites (emphasis added):

> ***transmitting a location information request message*** *including the source address of the received IP packet and receiving in response to said transmitted location information request message, information corresponding to the location of the user device*

The Examiner states on p. 5 of the Office Action that:

> "With regard to applicants argument that no location request message is transmitted, the examiner points to the database lookup of Tuck, as outlined above, and further seen in [0014]."

First, a "database lookup" is not the same as "transmitting a location information request message **including the source address of the received IP packet**" (emphasis added). There is no indication in the reference as to how a database lookup is accomplished, nor any indication that a transmitted "request message" includes "the source address of the received IP packet".

Further, [0014] of the Tuck et al. publication states (emphasis added):

> "...the router is able to identify the client node from its MAC address and can implement one or more suitable network and application policies that a network administrator may define for the client nodes".

Again, this is clearly using the "MAC address", as opposed to "a database lookup operation to retrieve **a geographic location stored in association with said edge router and port information**" (emphasis added).

For at least these additional reasons, claim 7 is patentable over the cited references.

The Examiner states on p. 2 of the Advisory Action that "Applicant further argues that the transmitting a request of claim 7 is substantially different [than] the database lookup of Tuck and claim 2. The examiner does not agree, as if he did, he would have restricted the claims." But, Appellant did not argue that claim 7 was "substantially different" than claim 2. There are distinctions between the claims, which speak for themselves. Rather, Appellant argues that both claims 2 and 7 are substantially different than the Tuck et al. publication, either alone or in combination with the other cited references.

The Examiner also states on p. 2 of the Advisory Action that "The claim does not state that the database lookup is given the edge router and port information as search criteria." Although the Examiner was referring to claim 2, and this was argued by Appellant in regard to claim 2 (above), claim 7 recites (emphasis added): "determining the location of the user device from edge router and port information obtained from an edge router, wherein the determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with said edge router and port information."

This even more clearly refutes the Examiner's contention that "The claim does not state that the database lookup is given the edge router and port information as search criteria" as it relates to claim 7.

For at least these additional reasons, claim 7 is patentable over the cited references, and its rejection should be overruled.

Group III: Claims 9 and 10

Claim 9 is representative of claim Group III.

Claims 9-10 stand rejected under 35 U.S.C. 103(a) as being unpatentable over the Tuck et al. publication in view of the Anderson et al. patent in further view of the Igval publication.

Claim 9 is patentable because, among other things, it recites the features indicated below:

> *(i) transmitting a location information request message including the source address of the received IP packet,*
> *(ii) receiving in response to said transmitted location information request message, information corresponding to the location of the user device determined from edge router and port information obtained from an edge router and a device identifier associated with the source address of said IP packet;*

Claim 9 is patentable for at least the reasons argued above in relation to claims 2 and 7.

Further, claim 9 recites:

> *comparing the received device identifier to a list of device identifiers corresponding to stolen devices*

which is not taught or suggested in **any** of the cited references. The Examiner on p. 4 of the final Office Action points to the Igval publication at paragraphs [0027 and 0028] as showing this feature. However, this reference doesn't "compare" anything to "a list of device identifiers corresponding to stolen devices". The Igval publication states at paragraph [0028], lines 20-23:

> "If at 454 the answer is no, then at 456 the data center 120 flags the postage meter 140b as lost or stolen and terminates the session."

Instead, this is the **opposite** of the claim 9 recitation. Rather than compare "the received device identifier to a list of device identifiers corresponding to stolen devices", the Igval publication uses other methods to determine that a device is stolen, and then flags it as such.

The Examiner states on p. 5 of the final Office Action that "Igval teaches flagging an ID as lost or stolen, and then will compare later IDs with the flagged ones". The problem is, the Igval publication does not teach or suggest this. The Igval publication does not even imply "comparing the received device identifier to a list of

device identifiers corresponding to stolen devices". The Examiner appears to be guessing that the Igval publication might, as a subsequent step, "and then will compare later IDs with the flagged ones". However, this is just a guess, and is not based on the reference itself.

For at least this additional reason, claim 9 is patentable over the cited references.

Claim 10, for at least the reason that it is dependent on patentable claim 9, is patentable over any combination of the cited references.

Therefore, the rejections of claims 9 and 10 should be overruled.

Group IV: Claim 11

Claim 11 stands rejected under 35 U.S.C. 103(a) as being unpatentable over the Tuck et al. publication in view of the Anderson et al. patent in further view of the Igval publication.

Claim 11 is at least patentable as it depends from patentable claim 9. Further, claim 11 recites the following features:

> *generating a message indicating the detection of a stolen device when said comparing step detects a match between the received device identifier and a device identifier in said list of device identifiers corresponding to stolen devices*

As the cited references do not teach or suggest the above feature, for this additional reason claim 11 is patentable over the cited references, and its rejection should be overruled.

Group V: Claims 12 and 13

Claims 12-13 stand rejected under 35 U.S.C. 103(a) as being unpatentable over the Tuck et al. publication in view of the Anderson et al. patent in further view of the Igval publication.

Claims 12 and 13 are at least patentable as they depend from patentable claims 9 and 11.

Claim 12 is representative of claim Group V.

Claim 12 is further patentable as it recites the following features:

> *wherein said generated message includes information indicating the geographic location where the identified stolen device is being used*

As the cited references do not teach or suggest the above feature, for this additional reason claim 12 is patentable over the cited references. As it depends from patentable claim 12, claim 13 is, at least for this reason, patentable over the cited references, and the rejections of claims 12 and 13 should be overruled.

Group VI: Claims 16 and 17

Claims 16 and 17 stand rejected under 35 U.S.C. 102(e) as being anticipated by the Tuck et al. publication.

Claim 16 is representative of claim Group VI.

Claim 16 is patentable because, among other things, it recites the features indicated below (emphasis added):

> *means for obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address, wherein determining the location of the user device further includes performing a* ***database lookup operation to retrieve a geographic location stored in association with edge router and port information****;*
>
> *a database of physical location information listing* ***physical locations authorized to obtain access to said service****; and*
>
> *wherein said means for determining an action to be taken includes a comparator for* ***comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided***

For the same reasons as argued above regarding claims 2 and 7, claim 16 is patentable over the cited references.

For at least the reason that it is dependent on allowable claim 16, claim 17 is patentable over the cited references, and the rejections should be overruled.

Group VII: Claims 32- 35

Claim 32 stands rejected under 35 U.S.C. 102(e) as being anticipated by the Tuck et al. publication.

Claims 33-35 stand rejected under 35 U.S.C. 103(a) as being unpatentable over the Tuck et al. publication in view of the Anderson et al. patent.

Claim 32 is representative of claim Group VIII.

Claim 32 is patentable because, among other things, it recites the features indicated below (emphasis added):

> *determining from said source address the* ***physical location*** *from which said IP packet was sent prior to delivery of the packet to the destination address;*
>
> ***comparing the determined physical location information to expected information*** *indicating the expected source of an IP packet; and*
>
> ***determining a reporting error when said determined physical location information does not match the expected physical location information***

For the reasons argued above in relation to claims 2 and 7, claim 32 is patentable over the cited references. Further the Examiner on p. 3 of the Office Action refers to the Tuck et al. publication at [0017] and [0119] in relation to claim 32. However, neither paragraph refers to "the expected physical location" in any manner. Also, neither paragraph refers to "determining a reporting error" for any purpose, but certainly not in response to "when said determined physical location information does not match the expected physical location information".

For at least these additional reasons, claim 32 is patentable over the cited references.

For at least the reason that they are dependent on allowable claim 32, claims 33 and 34 are patentable over the cited references, and the rejections of all three claims should be reversed.

Group VIII: Claim 36

Claim 36 is patentable over the cited references for at least the reasons argued above related to claim 9.

Additionally, claim 36 contains the feature:

> *receiving an IP packet including a source address wherein said IP packet is transmitted from a bracelet worn by a parolee and wherein said IP packet includes parolee identification information*

The Examiner does not allege that this feature is taught or suggested by any of the cited references. It would further not be obvious to link the features of "determining from said source address the physical location from which said IP packet was sent" with "a bracelet worn by a parolee". For at least this additional reason, claim 36 is patentable over the cited references.

Group IX: Claim 37

Claim 37 is patentable over the cited references for at least the reason that it is dependent on patentable claim 32.

Additionally, claim 37 contains the feature:

> *determining if said IP packet was sent at a predetermined time during which a location reporting message was scheduled to be transmitted*

None of the cited references teach or suggest this feature, nor does the Examiner claim that they do. Further, nothing in the references suggest relating their capabilities to "a predetermined time during which a location reporting message was scheduled to be transmitted", and therefore, it would not be obvious to alter the references to include such a feature. For at least this additional reason, claim 37 is patentable over the cited references.

VIII. Conclusion

In view of the foregoing, Appellant respectfully submits that the pending claims are in condition for allowance[1]. Accordingly, the Appellant requests that the Board reverse each of the outstanding grounds of rejection.

Any arguments made in this Appeal Brief pertain ***only*** to the specific aspects of the subject matter ***claimed***. Any arguments are made ***without prejudice to, or disclaimer of***, the Appellant's right to seek patent protection of any unclaimed (e.g., narrower, broader, different) subject matter, such as by way of a continuation or divisional patent application for example. To the extent necessary, a petition for extension of time under 37 C.F.R. 1.136 is hereby made and any required fee in regard to the extension or this amendment is authorized to be charged to the deposit account of Straub & Pokotylo, deposit account number 50-1049.

Respectfully submitted,

October 27, 2009

/Michael P. STRAUB, Reg. #36,941/
Michael P. Straub Attorney
Reg. No. 36,941
Tel.: (732) 936-1400

[1] As Appellant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Appellant's silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, ability to combine references, assertions as to patentability of dependent claims) is not a concession by Appellant that such assertions are accurate or such requirements have been met, and Appellant reserves the right to analyze and dispute such in the future.

IX. Claims Appendix

The claims currently on appeal are as follows:

Claim 2: A security method for use in a communication system, the security method comprising:

receiving an IP packet including a source address and a destination address;

obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address, and wherein determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with edge router and port information;

determining, as a function of the obtained physical location information, an action to be taken, wherein determining an action to be taken includes:

comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided.

Claim 3: The security method of claim 2, further comprising:

dropping said packet when said comparing does not result in a match between the obtained physical location information and the information listing physical locations authorized to obtain access to the service.

Claim 4: The security method of claim 2, wherein said service is one of a banking service, video on demand service and a music on demand service.

Claim 5: The security method of claim 2, further comprising:

forwarding said packet to the destination address when said comparing results in a match between the obtained physical location information and the information listing physical locations authorized to obtain access to the service.

Claim 7: A security method for use in a communication system, the security method comprising:

receiving an IP packet including a source address and a destination address;

obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address, including transmitting a location information request message including the source address of the received IP packet and receiving in response to said transmitted location information request message, information corresponding to the location of the user device;

determining, as a function of the obtained physical location information, an action to be taken, and

determining the location of the user device from edge router and port information obtained from an edge router, wherein the determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with said edge router and port information.

Claim 9: A security method for use in a communication system, the security method comprising:

(a) receiving an IP packet including a source address and a destination address;

(b) obtaining physical location information indicating the location of a user device which is the source of said IP packet, by:

(i) transmitting a location information request message including the source address of the received IP packet,

(ii) receiving in response to said transmitted location information request message, information corresponding to the location of the user device determined from edge router and port information obtained from an edge router and a device identifier associated with the source address of said IP packet;

(iii) performing a database lookup operation to retrieve a geographic location stored in association with said edge router and port information, and

(iv) comparing the received device identifier to a list of device identifiers corresponding to stolen devices,

and

(c) determining, as a function of the obtained physical location information, an action to be taken.

Claim 10: The security method of claim 9, wherein said device identifier is a MAC address.

Claim 11: The method of claim 9, further comprising:

generating a message indicating the detection of a stolen device when said comparing step detects a match between the received device identifier and a device identifier in said list of device identifiers corresponding to stolen devices.

Claim 12: The method of claim 11, wherein said generated message includes information indicating the geographic location where the identified stolen device is being used.

Claim 13: The method of claim 12, wherein said geographic location is a post office address.

Claim 16: A security device for use in a communication system in which IP packets are transmitted, the device comprising:

means for receiving an IP packet including a source address and a destination address;

means for obtaining physical location information indicating the location of a user device which is the source of said IP packet prior to delivery of the packet to the destination address, wherein determining the location of the user device further includes performing a database lookup operation to retrieve a geographic location stored in association with edge router and port information; and

means for determining, as a function of the obtained physical location information, an action to be taken;

a database of physical location information listing physical locations authorized to obtain access to said service; and

wherein said means for determining an action to be taken includes a comparator for comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided.

Claim 17: The security device of claim 16, further comprising:

means for dropping said packet when said comparing does not result in a match between the obtained physical location information and the information listing physical locations authorized to obtain access to the service.

Claim 18: The security device of claim 2, wherein said service is one of a banking service, video on demand service and a music on demand service.

Claim 32: A location verification method, the method comprising;

receiving an IP packet including a source address and a destination address;

determining from said source address the physical location from which said IP packet was sent prior to delivery of the packet to the destination address;

comparing the determined physical location information to expected information indicating the expected source of an IP packet; and

determining a reporting error when said determined physical location information does not match the expected physical location information.

Claim 33: The location verification method of claim 32, further comprising:

transmitting a message including information on the determined reporting error to a law enforcement authority.

Claim 34: The location verification method of claim 33, further comprising:

including the determined physical location information in said message.

Claim 35: The location verification method of claim 34, further comprising:

identifying the device transmitting said IP packet from a MAC address determined from a database associating said MAC address with said source address.

Claim 36: A location verification method, the method comprising;

receiving an IP packet including a source address wherein said IP packet is transmitted from a bracelet worn by a parolee and wherein said IP packet includes parolee identification information;

determining from said source address the physical location from which said IP packet was sent;

comparing the determined physical location information to expected information indicating the expected source of an IP packet;

determining a reporting error when said determined physical location information does not match the expected physical location information;

transmitting a message including information on the determined reporting error to a law enforcement authority;

including the determined physical location information in said message;

identifying the device transmitting said IP packet from a MAC address determined from a database associating said MAC address with said source address; and

including in said message information obtained from said IP packet identifying the parolee.

Claim 37: The location verification method of claim 33, further comprising:

determining if said IP packet was sent at a predetermined time during which a location reporting message was scheduled to be transmitted.

X. Evidence Appendix

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor is there any other evidence entered by the Examiner and relied upon by the Appellant in the appeal.

XI. Related proceedings Appendix

There are no decisions rendered by a court of the Board in any proceeding identified in section II above pursuant to 37 C.F.R. § 41.38 (c) (1) (ii).